



MICROS Customer Support

Remote Support Access Policy

A description of the policies and procedures relating to remote access to customer systems by MICROS Customer Support personnel. This document also includes MICROS's recommended connection and security methods as well as details on how PCI DSS, PABP and Sarbanes-Oxley requirements affect how MICROS customers are supported.

This document is provided by MICROS Systems, Inc. as a reference guide only and in no way implies that the recommendations described within will prevent unauthorized access to customer networks or systems. MICROS accepts no responsibility for the security of customer networks, systems, or applications. Please see the MICROS Maintenance Terms and Conditions section 21 for more details. Additionally, MICROS does not provide PCI DSS assessments or audits and cannot provide review of or approval for customer network security strategies or policies.

Document prepared by: Eric Seaman
Vice President, Customer Support
MICROS Systems, Inc. ©2009

Table 1: Change History

| DATE | DESCRIPTION |
|----------|--|
| 03.10.08 | Initial Draft |
| 05.09.08 | Updates based on feedback from VeriSign review |
| 09.23.08 | Updates to Approved Applications and Encryption Requirements |
| 04.21.09 | Updates to VPN Recommendations |
| 09.09.09 | Update to Approved Remote Support Applications/Solutions |
| 06.09.10 | Update to Approved Remote Support Applications/Solutions |

Contents

Overview 4

Intended Audience..... 4

Reference Documentation..... 4

Executive Summary..... 4

 MICROS Recommendations for Secure Remote Support Access 4

 MICROS Policies Regarding Secure Remote Support Access 5

Industry Requirements 5

 Payment Card Industry (PCI) Data Security Standard (DSS) 5

MICROS Recommendations 6

 1. Build and Maintain a Secure Network 6

 Firewalls 6

 User Accounts and Passwords 6

 2. Protect Cardholder Data 7

 Database Handling 7

 Transport Encryption 7

 3. Implement Strong Access Control Measures..... 7

 WebEx / Bomgar 8

 4. Regularly Monitor and Test Networks 8

 Track and Monitor All Access to Network Resources and Cardholder Data..... 8

Remote Access and Support Software..... 8

 Approved and Supported Applications:..... 8

 Not Supported or Approved: 9

Overview

In order to maintain compliance with specific industry requirements such as the Cardholder Information Security Program (CISP), Payment Card Industry Data Security Standard (PCI-DSS) and Payment Application Data Security Standard (PA-DSS), MICROS has developed standard policies controlling what methods are used to deliver remote support to customers from the MICROS Customer Support Center. This document describes the MICROS recommended connectivity and security methods and supported remote access applications and provides details on user account and password management.



Intended Audience

This document is intended for MICROS customers as well as MICROS Support, Implementation, Sales, and Account Management professionals, MICROS VARs and Service Partners and any other audience interested in the remote support policies and procedures used by the MICROS Support Center.

Reference Documentation

- The Payment Card Industry Security Standards Council (PCI-SSC) web site is available at: <https://www.pcisecuritystandards.org/>
- The latest version of the Payment Card Industry Data Security Standard (PCI-DSS) is available at: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
- A listing of Qualified Security Assessors (QSA's) is available from the PCI-SSC web site at: https://www.pcisecuritystandards.org/qa_asv/find_one.shtml
- A copy of the Payment Card Industry (PCI) Self-Assessment Questionnaire from the PCI-SSC is available at: <https://www.pcisecuritystandards.org/saq/index.shtml>
- General information on PCI compliance validation and requirements are available from VISA's web site at http://usa.visa.com/merchants/risk_management/cisp_merchants.html
- MICROS related PCI information is available at <http://www.micros.com/ServicesAndSupport/InformationSecurity/>

Executive Summary

MICROS Recommendations for Secure Remote Support Access

1. Customers should implement and maintain secure network infrastructure and policies such as firewalls, Network Address Translation (NAT), Access Control Lists (ACL's), individual user-account-based authentication, and routine password rotation.
2. Customers are advised to implement secure methods for remote support access that comply with the terms of the PCI-DSS.
3. Customers should implement methods for logging user access to their networks and system(s) consistent with Section 10 of the PCI-DSS.

4. Remote access applications and user accounts/passwords configured for use by MICROS Support should be enabled only when needed for remote access and should be disabled or removed immediately afterward. For security purposes, MICROS discourages the use of persistent open communications between your MICROS system and any public networks.
5. In addition to standard access controls, user accounts configured for remote access should include only those access rights required for the service/support being provided and should be robustly audited.

MICROS Policies Regarding Secure Remote Support Access

1. MICROS will only provide remote support via solutions that have been tested and approved by MICROS Customer Support. Solutions not approved and supported by MICROS Customer Support can be nominated for approval through your Account Manager or Account Representative. A testing and validation fee may be charged to complete the approval process. Additional costs may be included if non-standard or unsupported software is required.
2. MICROS Customer Support will not store or manage user account information or passwords for customer systems or applications. It is recommended that customers use unique and strong user-based accounts and passwords for network and application access. MICROS Customer Support is unable to provide assistance for issues involving lost or forgotten passwords or user account information.
3. MICROS Customer Support does not provide network configuration, implementation, or consultation services. Customer network and network configuration support is not provided by MICROS Customer Support.



Industry Requirements

The PCI Security Standards Council (PCI-SSC) was formed in 2005 by Visa, MasterCard, American Express, Discover and JCB to develop industry standards relating to the handling and storage of credit card data and credit card customer information. These standards comprise the Payment Card Industry Data Security Standard (PCI-DSS). The PCI-DSS details specific requirements relating to network security and access control. The following is a summary of those requirements which impact how MICROS provides remote support to its customers. Complete details on PCI-DSS requirements can be found at www.pcisecuritystandards.org and should be reviewed in detail by each customer with their individual PCI-DSS Qualified Security Assessor (QSA). *MICROS does not provide PCI-DSS assessments or audits and cannot provide approval for customer network security strategies or policies.*

Payment Card Industry (PCI) Data Security Standard (DSS)

PCI-DSS requirements are applicable to any networks or systems where credit card Primary Account Numbers (PAN) are stored, processed, or transmitted. These requirements apply to all MICROS products with the optional Credit Card (CA/EDC) module installed and active and

applies to all “system components”. The PCI Council defines System Components as “... any network component, server, or application that is included in or connected to the cardholder data environment.” Please refer to the PCI-DSS for more detail.

The PCI-DSS is comprised of 12 General Requirements grouped in 6 Sections.

| SECTION | GENERAL REQUIREMENT |
|---|---|
| Build and Maintain a Secure Network | 1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords or other security parameters |
| Protect Cardholder Data | 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks |
| Maintain a Vulnerability Management Program | 5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications |
| Implement Strong Access Control Measures | 7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data |
| Regularly Monitor and Test Networks | 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes |
| Maintain an Information Security Policy | 12. Maintain a policy that addresses information security |

MICROS Recommendations

The following recommendations are provide as a guideline that should be followed to help ensure MICROS’ support personnel are able to provide you with remote support assistance without compromising your Information Security Policy.

1. Build and Maintain a Secure Network

Firewalls

MICROS recommends that all customers implement and maintain network access control appliances and/or software to control access to and from customer networks and systems (firewalls). Firewalls should include the use of Network Address Translation (NAT), Packet Filtering, Access Control Lists (ACL) and/or Application-Layer firewalls.

User Accounts and Passwords

All system default user accounts and passwords or user accounts and passwords created during the installation and configuration of your MICROS product(s) should be removed, disabled, or passwords changed to unique, complex values as per the terms of the PCI-DSS. MICROS will *not* maintain or store user account information, including passwords, for your

system. MICROS Support will not create or modify any user accounts or account passwords on your system nor does MICROS Support have dedicated user accounts or “back door” accounts available. If when contacting MICROS support a customer is unable to provide a login and password for access (if needed) to the MICROS application, database, or Operating System, remote support cannot be provided.

MICROS recommends that unique user accounts with strong passwords are used for all users including any user accounts assigned for use by the MICROS Support Center. User accounts provided to MICROS Support for remote support access should be disabled when not in use.

2. Protect Cardholder Data

Database Handling

Cardholder data is stored in a highly encrypted format within your PA-DSS Validated MICROS product’s database (sensitive Track Two data is not stored by MICROS PA-DSS Validated products). From time to time it may be necessary for MICROS Support to obtain a copy of your database for testing or trouble-shooting

purposes. In such cases, MICROS will transfer a copy of the database via secure connection to a dedicated test machine within the MICROS Support Center. Once testing and/or trouble-shooting has completed, the database and any data generated from the database (i.e. reports, data exports, etc.) will be destroyed. Disk based data will be destroyed using secure delete methods consistent with the data removal process defined by the National Industrial Security Program Operating Manual of the US Department of Defense. Physical media used to store customer data (i.e. CD, DVD, diskette, etc.) will be destroyed through the use of a shredder.



MICROS Customer Support will not accept databases from customer via email or unsecure file transfer. Databases can be mailed to MICROS Customer Support only by utilizing a tracking-based shipping method that requires an accepting signature (i.e. FedEx, UPS, USPS Certified mail, etc.).

Transport Encryption

Connectivity methods provided by customers must be capable of providing at least 128 bit encryption at the transport layer (SSL or IPSEC).

3. Implement Strong Access Control Measures

MICROS recommends that each customer provide remote access to be used by MICROS Customer Support via PCI-DSS compliant methods. Allowing access to your network and/or

systems using unsecure methods or methods not conforming to PCI-DSS standards can leave you open to breach and loss of sensitive data as well as fines and other costs.

Implementation of networks, network configurations, and network security are the responsibility of the customer. MICROS does not provide network planning or development services.

WebEx / Bomgar

MICROS currently utilizes WebEx's Support Center™ and or Bomgar™ products for all remote support tasks. WebEx & Bomgar are on-demand, secure, remote access applications. A "Support Session" can only be started via a cooperative exchange between the customer and a MICROS Customer Support agent. Once a Support Session is started the customer must grant access to either the entire system or an individual application(s). Application level access must be provided to the Support Agent by the customer as well.

4. Regularly Monitor and Test Networks

Track and Monitor All Access to Network Resources and Cardholder Data

MICROS recommends that customers implement methods for logging user access to their system(s) consistent with Section 10 of the PCI-DSS. Logging should be enabled both within the MICROS application(s) and at the Operating System level to ensure that all user access can be audited. See the Payment Card Industry Data Security Standard (PCI-DSS) document or consult your PCI Consultant or Qualified Security Assessor (QSA) for more information.

Remote Access and Support Software

MICROS will provide remote support to customers using WebEx or Bomgar for customer sites with Broadband access or PCAnywhere for customers with only traditional dial-up modem access. PCAnywhere will not be used to initiate broadband or internet based remote support sessions.

Approved and Supported Applications:

1. WebEx Remote Support
2. Bomgar
3. Symantec PCAnywhere version 12.5 or later with the security configuration options set per MICROS recommendations (as outlined in the MICROS document titled Secure Configuration of PCAnywhere) including:
 - a. Symmetric or Public Key encryption enabled
 - b. Logging enabled
 - c. Account Lockout enabled
 - d. Prompt to Confirm Connection enabled
 - e. Use of unique user account and password for each support session
 - f. PCAnywhere Host must be disabled when not in use
4. Other remote access tools or applications reviewed and approved by MICROS in writing

Not Supported or Approved:

1. WebEx Remote Access Solution (a.k.a. SMARTech)
2. Direct unsecured internet connection via PCAnywhere, VNC, Microsoft Remote Desktop, or other remote access tool
3. Any remote access method that does not require the customer to grant access at the time the connection is being made to a system or network.